What are the Symptoms of a Computer Virus?

File Disappears—A file, or a portion of a file, disappears from a hard disk or floppy.

File Appears—A mystery file appears.

Changes in Data—Data is deleted, added, or moved.

Disk Space or Memory—Unexplained decreases in the amount of memory, or, the hard disk fills up faster than normal.

"A" Drive Access Light Flashes—The "A" drive light flashes when the drive is empty.

Slow System—The system takes longer to boot up, response time lags, it takes longer to access the disk drive or to load a program.

Unusual Video Displays—Strange messages, peculiar graphics, scrolling of odd parts of the screen, the unexpected appearance of "bouncing balls," letters falling down the screen, or the display of the word "GOTCHA."

Rebooting Workstations—Workstations unexpectedly reboot when specific programs are run.

Time Stamp Changes—Unexplained changes in the Update Timestamp of programs of the operating system or utilities.

Division of Information Technology Services
6000 State Office Building
Salt Lake City, Utah 84114
Phone: 801-538-3833
FAX: 538-3622

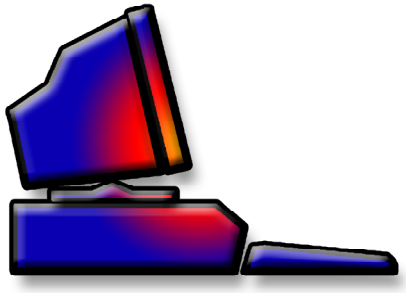
ITS Customer Support
801-538-3440 or 800-678-3440
http://its.utah.gov/services/support/helpdesk.htm

ITS Computer Security Office
http://security.utah.gov

ITS Internet Site
http://its.utah.gov

ITS Customer Driven Technology
Information Technology Services

Utah!
Where ideas connect



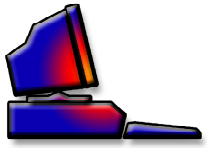
Computer Viruses

What Should I Know?

What Should I Do?

What is a Computer Virus?

A computer virus is a program that replicates itself and attaches itself to other programs. Malicious viruses sneak into systems and attack files, directories, and operating code, without human intervention or knowledge.



What Should I Do If I Suspect that My System is Infected?

The longer a computer virus goes undetected the greater the potential is for loss.

STOP using the system immediately.

POST a sign on the system advising other users not to use the system.

CONTACT Information Technology Services Customer Support at 801-538-3440.

CAUTION: DO NOT ATTEMPT to run your programs on another system. If your programs are infected, you will spread the virus.

DO NOT ATTEMPT to recover your data from your backup disks without first contacting ITS Customer Support. Any attempt to restore your data and programs without first removing all copies of the virus from your system could result in the contamination of your backup copies and drastically reduce the possibility of a successful recovery.

There are Two Main Types of Viruses

Boot Infector

This type of virus writes itself on the sector containing the instructions for booting the system.

File Infector

This type of virus attacks executable files, most often .com and .exe files. When the program is run, the virus executes first, then the virus writes itself into memory and then attaches to other programs.

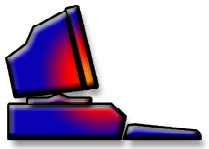
Other Virus Techniques

Trojan Horse

A Trojan Horse is a program that looks normal but contains harmful code hidden within. These programs are designed to do things that the user of the program does not intend to do. These types of programs are most commonly used to commit program based frauds and for introducing computer viruses into systems.

Blended Threats

Evolving attacks and network subversion methods, known as Blended Threats, combine hacking, DoS, and worm-like propagation. External attacks are more prevalent than internal attacks for proliferating vulnerabilities, but there is a growing need to protect against both internal and external attacks. Blended Threats are often spread without human interaction.



Logic Bomb

A Logic Bomb is a programing technique used to execute malicious code when some predefined condition occurs. The malicious code can be triggered by a change in a particular file, by the number of times a file is updated, on a particular date (this variation is commonly known as a time bomb) or any number of other circumstances, which can be imagined. If a computer virus uses this logic bomb technique to keep its destructive code dormant, and remains undetected for any extended period of time, numerous generations of backup copies of both data and programs could be infected, making recovery extremely difficult.

WORM

The acronym WORM stands for Write Once Read Many. These programs were originally developed to constructively tap into unused network resources, usually storage space or programs. The WORM program searches the network computers without the approval of the system's owners and can insert itself without being run or executed by a user. By claiming all available space and processing capabilities, a WORM program can tie up all of the computing resources of a system and essentially render it useless. Unlike a virus, which attaches itself to another program, the WORM program is self-contained and does not need to copy its code into another existing program on the system.